Meltdown

O Meltdown consiste em quebrar um mecanismo de segurança dos processadores da Intel que previne aplicativos de acessarem a memória reservada ao kernel do sistema operacional. Ele se chama assim porque "derrete" (melt, em inglês) a barreira de defesa dos chips.

Como o kernel é o responsável por praticamente tudo, servindo como ponte entre os softwares e o hardware da máquina, a falha é considerada grave. Em teoria, ela permite que um aplicativo comum (inclusive um malware ou até mesmo um código em JavaScript rodando no navegador) tenha acesso a senhas e outras informações restritas.

Spectre

O nome do Spectre está relacionado à causa do problema, que é a execução especulativa (speculative execution, em inglês). Para acelerar o desempenho dos softwares, os processadores modernos tentam adivinhar qual código será executado em seguida. Caso a previsão esteja errada, o resultado é simplesmente descartado; caso esteja certa, há uma economia de tempo aqui.

No entanto, a tecnologia também pode induzir um processador a executar uma operação "adivinhada" que não seria executada em condições normais. Isso permite que um aplicativo vaze uma informação confidencial para outro aplicativo, quebrando vários mecanismos de segurança de softwares, como o sandbox do Chrome, que separa as abas de sites e o resto do sistema operacional, por exemplo.

PortSmash

O SMT permite que um processador multicore agende tarefas (as threads) de forma muito mais eficiente, com cada núcleo processando vários processos ao mesmo tempo. No entanto, os códigos executados em threads distintas podem ser trocados entre si, dependendo da aplicação que está sendo rodada.

O PortSmash explora essa particularidade do SMT para o ataque: o código malicioso precisa ser rodado no mesmo núcleo ao mesmo tempo que um processo legítimo em outra thread, injetando fragmentos para alterar uma tarefa e forçar o processador a vazar dados criptografados, que poderão ser recuperados. Como o hardware não foi preparado para um ataque de tão baixo nível, o processador é incapaz de impedir a invasão.

Fontes: https://canaltech.com.br/seguranca/chips-intel-e-bugs-spectre-e-meltdown-afinal-o-que-acontece-e-como-resolver-106130/

https://meiobit.com/392554/intel-portsmash-nova-vulnerabilidade/